Project:
The Landscape and Isobars of European Values in Relation to Science and New Technology (ValueIsobars)

Project number:
230557

Title of deliverable*:

Joint publication draft:
"Biometrics technologies and their influence on societal values and conceptions of identity"

Work package:
WP5

Author(s):

Laurens Landeweerd, Julian Kinderlerer, David Townend, Maria-Eduarda Gonsalves

Partner (institution):
UNIMAAS

Deliverable 5.3a

Date: 14 februari 2012

Biometrics technologies and their influence on societal values and conceptions of identity

Laurens Landeweerd, David Townend, Maria Eduarda Gonsalves (?)

Abstract
Biometrics may aid in countering threats of terrorism and they may aid in identifying criminals. They may also aid in avoiding mistakes in an increasingly complex health care system. They can facilitate in making access restriction to sensitive research materials more watertight, and help protect the interests of industry and corporate business. Still, all these beneficial applications come at a risk, specifically with regard to the justification of the proposed use, and with regard to whether one can contain their use to its proper and intended purposes. Passengers name records and other biometrics data are retained for anti-terrorist purposes, but this may be damaging to the privacy of the individuals concerned. As a result, the discourse on biometrics technologies has increasingly emerged as a tension area between security and privacy. In the private sector, uses of personal data that potentially also pose a threat for personal privacy. Problems include multiple uses of data collected by private companies such as banks, insurance companies and uses of information for marketing purposes. And although the consequences of misuse of data for security purposes are often seen as more problematic, commercial misuse of biometrics data is also widespread a problem: abuse of biometrics data include unauthorised disclosure of medical information or unauthorised use for targeted advertisement. The tension between the right to privacy and issues of security emerged as the most dominant field of concern in the past ten years. Due to the dominance of these values and the perceived conflict between the two, other moral aspects of the introduction of biometrics technologies in various areas have been neglected. This paper aims to provide for a more articulated account of the underlying moral aspects and societal drivers for the implementation of biometrics technologies, in order to contribute to more well-argued policies.

1. Introduction

'Biometrics' is an umbrella term. It refers to all technologies that identify a person on the basis of his or her biological traits or behavioural characteristics. In the past, biometrics technologies were mostly applied to criminal investigation. One of the first of such application of biometrics was fingerprinting, and its use dates back to 14th century China (although in Europe their use was not discovered until the 19th century) (Liberatore 2007). Currently, they are presented as a means to tackle a much wider range of recent and less recent social problems by 'protecting and managing the uniqueness of identity' (Ajana 2010). Social problems that are expected to be countered by a range of biometrics technologies include identity theft and fraud, crime and terrorism, illegal work and employment, the efficient governance of asylum, immigration and social welfare (Ajana 2010). Digitalisation has caused an exponential growth in the number and spread of biometrics technologies. They also render the body more 'readable', in terms of digital codes and ciphers (van der Ploeg, 1999). The threat of terrorism or criminality forms an important driver to increase the application of biometrics technology and other forms of surveillance, carrying along both societal benefits and threats to certain basically held values such as autonomy and privacy. However, due to the conceptual vagueness of values such as 'security', 'privacy', 'autonomy' and 'identity', the debate on biometrics technologies and their various uses has become a trench war between governments and specific NGO's and other interest groups in a semantic minefield. Clarification of such concepts may help rationalise policies on the introduction, spread and containment of biometrics technologies and data more.

In order for a technology to qualify as a biometrics technology, one first needs to be able to *measure* the biological traits or behavioural characteristics in question; secondly, one needs to measure a biological trait or behavioural characteristic that is *common* (having a face, having a voice); thirdly, the biological trait or behavioural characteristic must be *unique* for every person and fourthly, the biological trait or behavioural characteristic must remain *permanent* over time (a face changes, but the distance between the eyes not for example) (Mordini & Massari 2008).. With these four criteria, those technologies that can be identified as biometrics technologies are quite diverse. They vary from recognition through fingerprints to genetic data, from automatic facial recognition software to pictures and they include iris scans, hand geometry, face and ear shape recognition, signature dynamics, voice recognition but even computer keystroke dynamics can now be added to this list.

The European Council expressed its intention to use biometrics to counter security threats with regard to visa policy in to counter illegal migration (European Council, 2003) and security in the context of the fight against terrorism (Declaration on Combating Terrorism of March 2004 and Presidency Conclusions of the Brussels Council of December 2004). The policy measures taken to implement biometrics technologies were delegated in part to national governments, some of which were more active to follow up than others. The introduction of various biometrics approaches such as the biometrics passport was calibrated closely with similar policy decisions in the United States. Industry seized the opportunity to make use of this development whilst the ensuing public controversies focused on issues of economic cost and issues human rights (most notably privacy). Non-governmental organisations such as Amnesty International, Privacy International and Statewatch and have expressed their criticism of the current implementation of biometrics and are also critical of their effectiveness in enhancing security[1].

Article 29 deals with data protection, and biometrics data have been kept under close scrutiny over these past years by a number of independent organisations such as the Article 29 Data Protection Working Party (2004) or the Joint Supervisory Authority of Schengen (2004). They both perceive of major issues with regard to the use of biometrics data for other than the originally intended purpose. Public awareness of the nature, uses, perceived benefits and harms of biometrics technologies is increasing in several EU-member states due to their large scale introduction of biometric passports. As a result, public debate also increases. One of the main topics debated is the problem of function creep, combined with the issue that surveillance may be used for goals different from countering security threats. Since the introduction of a biometrics passport has gone outside of, and in some cases even counter to, democratic scrutiny, these debates are not likely to fall silent in the near future. The invisibility of those that execute the surveillance only adds to societal concerns and tensions. The fact that individuals do not have open access to what happens with their personal data creates an atmosphere of mutual mistrust as the public sphere was and still remains completely disconnected from the arena of political decision making. One concern is the fear for the emergence of a so called 'surveillance society', in which governments and other institutions control their subjects through a variety of surveillance technologies and in which such surveillance would, instead of being a means to keep track of crime and terrorism, be a goal onto itself. Another issue is that data collected for one specific purpose may unintentionally or without authorisation be used for entirely different purposes. This shift of function, also referred to as 'function creep' (Woodward et al. 2001-I) does not merely pose a problem for privacy in security applications of biometrics, but also in commercial applications. In the public sector, uses of personal data that potentially pose a threat for personal privacy include the so called 'war on terror and criminality'. A third concern is that personal autonomy is frustrated through the use of biometrics technologies. With regard to all these concerns, the tension area between security and privacy plays a major role.

The debate on the introduction and spread of biometrics technologies is framed in terms of trade-offs between privacy (and the connected right to autonomy) and security. Security and privacy are seen to be at odds, in specific with regard to international traffic and internet- and public-space-related identification technologies Until recently however, security on the one hand and autonomy and privacy on the other were not as automatically seen to be at odds. Security was a means to safeguard citizens against criminality and terrorism, thereby safeguarding safety and autonomy, and the marginal nature with which security intervened in personal life (showing a passport with a photo when on an international trip) and bodily integrity (mostly only breached when suspected in something crime-related) was not sufficient an issue to cause public concern. This has changed in a very short time span of some ten years under the pressure of both public and political concern over terrorist threats and the increase of the use of new infrastructures and technologies to counter such threats. In legal, political and societal discourse on biometrics, the balance between security and privacy has emerged as the dominant discourse.

Governments usually defend the introduction of policies for the use of biometrics seen their use to counter terrorism and criminality, whilst interest groups in society claim they harm privacy. Governmental response to this criticism usually centres on four standard arguments (Alterman 2003; pp. 141):

---

[1] E.g., Amnesty International, "Concerns in Europe July–December 2001", http://web.amnesty.org/library/index/ENGEUR010022002; Statewatch: "Biometrics: The EU takes another step down the road to 1984": http://www.statewatch.org/news/2003/sep/19eubiometric.htm; Privacy International: "PI forges coalition calling on European Parliament to stop mass fingerprinting proposal": http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-85336.

(1) The "technical limits" argument: in a large population the technology has limited capability to identify a particular individual.
(2) The "balkanization" argument: information remains local and restricted because no interoperability standards exist. [this belief expresses a false sense of security with regard to function shift or function creep]
(3) The "cooperation" argument: the technology cannot easily be abused because identification requires cooperation.
(4) The "security" argument: the template algorithms are secure because biometrics vendors have a proprietary interest in keeping them confidential.

These four arguments are not valid for most biometrics technology [ref and/or explanation]. Although the threats of terrorism or criminality is not to be taken lightly, the strategies to counter these threats may not be as effective as they purport to be, and they may find other uses that are not connected to these original goals. The effectiveness of these measures to combat terrorism or to fight crime is contested. Because of the risk of function creep, the broad application of surveillance technology such as biometrics may find other uses that were neither the original intention of the users nor consented to by those whose information is gathered and retained. This may lead to a surveillance society where privacy is increasingly eroded away.

2. Privacy and Security

Privacy can briefly be defined as the right not to be interfered with in ones personal and bodily integrity, personal conduct and freedom of movement. An important value-related issue here concerns the separation between public and private. There are two problem areas with regard to privacy and the use of biometrics technologies: the use of biometrics technologies may lead to the creation of a 'surveillance society', in which any citizen may feel to be criminalised, merely in the light of purposes of security that are often felt to be abstract. Biometrics technologies have a potential both in their nature and their use to harm the principled right to privacy. Biometrics technologies render the body and the person transparent to the organisation that uses the data in question. The extent of this transparency differs per technology and per goal. Biometrics technologies can be used as a mechanism of control over subjects, be it legitimate and justified or not (depending on the use these can be citizens, illegal aliens, clients, patients, employees, or customers). And without the knowledge or agreement of the subject in question, third parties may use the information in question for goals the subject in question did not intend or support.
In the case of biometrics, it is quite clear what values are at stake. Biometrics is very much an issue of safety versus privacy. More in detail, this includes the following issues:

- Psychological problems of feeling surveyed (a virtual panopticon)
- Avoidance of surveyed spaces
- Privacy in the public space
- False reliability, ritual senses of security
- Mistaken identity and its consequences
- Oppressed groups

The impact of the introduction of different biometrics technologies is however unclear, and the consequences on how society changes may be enormous. Security may become a goal in itself, rather than an instrument to prevent specific harms, an effect may be a shift in the mentality of governments and societies towards a surveillance-society. Is it the safety "culture" and the mindset of those working with the topic that is problematic? Are they too much rigged to only see issues of risk and safety as relevant, ignoring issues of dual-use and security?

In the European Convention on Human Rights, privacy and personal integrity are not regarded as absolutes (in contrast with for example the right not to be tortured). Security is regarded as negotiable as well, albeit to a lesser extent. Both should be given attention, rather than abandoning the one value of in favour of the other (Liberatore 2007) and where there is a conflict between these two, either, or both need to be compromised to a certain extent. But since there is a wide variety of biometrics technologies, it may well be that some are less damaging for principles of privacy, and personal integrity than others. Hence, it is important to see whether and why such a trade-off is indeed being made, and whether it is a necessary trade-off (Liberatore 2007).

EU Regulation of biometrics

- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States amended by Regulation (EC) No 444/2009 of 28 May 2009

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Related instruments:

- Charter of Fundamental Rights of the European Union (Articles 6º, 7º and 8º)
- Council Decision of 8 June 2004 establishing the Visa Information System (2004/512/EC)
- Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas

3. The Deeper Significance of Privacy and Security

Privacy has come to be construed as a public good that can be traded for access to goods, information, transportation and security. With regard to security, biometrics technologies in specific demand a trade from individual citizens for access to public spaces and transportation. Due to the top-down introduction of biometrics technologies, specifically in their use for non-commercial purposes, this is a trade off that can no longer be circumvented by choosing for alternatives[2]. That is, one only has access to such goods if one is prepared to give up certain aspects of one's private life and private identity. Societal discourse however revolves around the question why it would be problematic to no longer be able to hide certain aspects of one's person. In other words, someone who has something to hide must be up to something, so why would one object? In the tone of such debates, an important aspect is lost: how is governmental and corporate business' interest in our personal data motivated? Not having anything to hide is after all something different from being open to being scanned, surveyed and kept under close watch all the time, whether the means to do so are pronouncedly present and bothersome (on airports for example) or hidden and invisible (in facial recognition software when combined with security cameras for example). After all, apart from the explicit rationale and motivation of their introduction, the surveyors themselves and their motivations do remain hidden, and the process of biometrics data exchange is not transparent on both sides. Individual citizens do not have access to their personal data nor do they have a view on what happens to such data. This means individual citizens cannot exert any control over their virtual identities. This does not only hold effects on public acceptance of the biometrics technologies involved, it also carries along serious issues of democratic legitimacy.

It appears that the introduction of biometrics technologies has challenged the traditional notion of security. Security was unproblematically seen as one of the preconditions of personal liberty. But as a result of the invasiveness of biometrics technologies as well as the non-transparency of how the resulting data is collected and used, it is now felt to be at a par with personal freedom. This means that, due to biometrics' effects on issues of privacy and data protection, the value of security is gradually becoming reified as something that stands in opposition to personal freedom rather than as one of its preconditions.

The introduction of biometrics technologies has an impact on our notions of individual identity: the identity we choose to attribute to ourselves is cross-cut by different technological notions of our identity that may stand in stark contrast and even come into conflict with our own 'sense of self'. We live

[2] The Rathenau report 'Check in – Check out' specifically analyses such issues of identity management with regard to transportation (Rathenau 200?).

in an environment that has come to be intrinsically mediated by technology. In that sense, the human ecosystem, as F. Brom termed it, has become a technotope. Any notion of an environment free of such technological intervention or mediation has become a romantic fantasy. Still, where individuals no longer feel comfortable with certain aspects of this pervasive presence of technology in daily life, the question forces itself to the foreground whether we as citizens are indeed at home in this environment. At that stage, the technology-mediated net we are constantly embedded in, through mobile internet, mobile phones, public transport cards, TomTom-systems or surveillance cameras becomes a web in which we may feel ensnared rather than enabled. Specifically the issue of privacy gives cause to such feelings of entrapment, and therefore to wide public or societal concern.

The notion of a 'core identity' to which only the subject itself has some kind of privileged access is outdated. Our technotope structures, enables and restricts our access the management of our identities, be they professional, personal or as a citizen. In this sense, the tendency of governmental bodies and macro-organisations to control individual behaviour and public life needs to be steered in a responsible fashion. If one frustrates individual life in society, this will bar individual freedom to creatively shape one's life and daily practices. In this sense, security is a two-faced daemon: although being preconditional for individual liberty in cases of extreme threat, it can evenly pose a threat to individual liberty if introduced as common practice in daily life. If those technologies that shape our environment restrict our access to goods, information, transportation, access to public places, they restrict our sense of belonging in this environment and therefore our sense of self. And if we no longer hold any individual control or authority over what happens to our personal date, this restriction affects and restricts our identities in an even more direct sense. Then, our technotope will be perceived of as totalitarian-technocratic in character rather than a 'natural' environment.

4. Proportionality of Implementation

The protection of privacy might hamper security measures in the light of terrorism but it might also hamper the prevention of abuse of public service and the freedom enjoyed in the public sphere. It is difficult to balance these two opposite types of principles and values. On the other hand, invisibility is increasingly put forward by the authorities as a potential threat in modern society. The ability to identify persons more easily may aid in reducing the risk of a terrorist attack, it is argued. And although biometrics technologies, due to their technological and digital nature, may appear to be more effective than non-technological strategies, they may only lead to an illusion of safety, whilst carrying along serious harms to privacy and personal freedom.

In sum, there is a need for a proper assessment of the effectiveness of the technologies involved and an assessment of possible unexpected or less predictable harmful side effects. One should go further than demonstrating there are no harms involved, there should be a positive assessment of what benefits are served. The goal of countering terrorism may be overreached when the means to achieve security go beyond this and the function of biometrics technologies shift to general control over citizens in modern society. Protecting national and international security in name of the safety of its citizens may lead to uses without explicit purpose, and without consent and it may serve to inadvertently enhance global tensions with regard to terrorism rather than decrease them. In the extreme, these uses might lead to a criminalisation of innocent citizens and damage values such as personal freedom, bodily integrity, the possibility to move freely in the public sphere and privacy.

Connected to all tension fields with regard to biometrics technologies is the issue of whether the use of such technologies is proportional or disproportional with regard to the intended goals. Can one render the person, body and private lives of all citizens transparent merely to decrease the risk of a terrorist attack? After all, before 9-11 there was an equally serious threat of terrorism in several countries in Europe, including the UK (the IRA), Spain (the ETA) etc, and in spite of these threats, privacy was not as extensively disrupted as may become the case with the use of biometrics technologies. And is health care efficiency worth any price? Can one balance the principles involved at all, or are they to be seen as absolute values?

The implementation of biometrics is taking place without much attention to whether it is a suitable option to increase security. It may well be that, for example, infiltration and close monitoring of terrorist groups yields much more effective results than a widespread introduction of biometrics technologies. Biometrics may amount to a buckshot-approach to kill a fly. Up till now, the societal debate mainly focused on whether biometrics has a negative impact on fundamental right, whilst critical questions may need to be posed one stage earlier. An important pragmatic issue in this respect is whether the

specific biometrics technology is a viable option: it often seems to be taken for granted that any biometrics technology will be effective, whilst there will be strong differences between the options at out disposal. Choosing between such options should be motivated by whether they result in a 'Big-Brother' approach of security, or pose a less invasive option to enhance security. This is not only an issue dependent of the biometrics technology in question, but also of their implementation in practice, their use, and the organisations, groups and individuals responsible for their execution. The rate of error (erroneous identification) is one of the most crucial factors is weighing different technologies and their uses.

Current policies on biometrics are specifically European in nature. As Liberato states: "With regard to biometrics, so far the issues is distinctly "European" (namely in terms of EU-level decisions, European response to US initiatives) – with some "variations on a theme" such as the focus in the UK on the introduction of ID cards, in Germany on the costs of biometrics and different views on its benefits within the governmental coalition, in France with regard to the broader context of rights on the Internet, in Italy where problems for privacy are strongly pointed out […]" (Liberato 2007). This very pluralism in current introductions of biometrics technologies and their connected values is also to be seen as specifically European. This plurality should be respected on lower levels as well as on such a national level. Democratic involvement and democratic expertise may contribute to the complexity of decisions at stake. It would allow for an incorporation of a plurality of perspectives and different forms of tacit knowledge in policy making as well as technological innovation agendas. Public debates, stakeholder interaction and internet-based diffusion of and response to information would enhance public debate on biometrics. This would form a strong basis for a process-based technical, social, economic, ethical and legal assessment. It would increase the accountability of the parties responsible for the implementation of various biometrics technologies – one of the major problems in the public eye – and it would enhance the effectiveness of the measures in question.

5. Conclusion

If there is no societal input in current applications of biometrics technologies for security purposes, an opportunity is missed for a more dialogical approach, therefore lessening the quality of such control systems, and increasing the establishment of s surveillance society that is no longer aimed at creating a secure environment for its citizens but takes surveillance as a goal in itself. Public support and public management of virtual identities is adamant for an introduction of biometrics technologies that is rational, democratically legitimate and effective.